



AHCCCS

Arizona Health Care Cost Containment System

Committed to excellence in health care

AHCCCS

Electronic Claim Submission Requirements

Information Services Division

December, 2003 Edition

Intended Users

The Electronic Claim Submission Requirements manual is distributed to any qualified entity who wishes to submit fee-for-service claims electronically to the Arizona Health Care Cost Containment System Administration (AHCCCSA), and is intended to provide the reader with information covering all aspects of Electronic Claims Submission (ECS), from sign-up and certification procedures, to the required file specifications.

Manual Contents

The Electronic Claim Submission Requirements manual includes the following sections:

Problem Resolution

Includes instructions regarding contacting the AHCCCSA with any problems relating to the electronic submission of claims.

Registration Requirements

Includes instructions on how to register prior to submitting claims electronically to AHCCCSA.

Submitting Claims Electronically to AHCCCSA

Includes information on AHCCCSA's electronic claims technical environment, products which may be used to submit claims electronically, as well as step-by-step instructions on how to submit electronic claims.

Submission Requirements

Includes volume and frequency limits, which must be adhered to when submitting electronic claims.

Testing

Includes information on the testing requirements, which must be met prior to any production claim being accepted electronically by AHCCCSA, as well as the testing procedures, which must be followed.

Attachments

Includes information regarding the impact of electronic submission of claims on required claims attachments such as medical documentation, EOBs, Sterilization Consent forms, etc.

File Specifications

Includes the file layouts for electronic claim submission. AHCCCSA uses the NSF (Medicare) standard format for the UB92 and HCFA-1500 forms, and the NCPDP standard for Universal (pharmacy) forms.

In addition, this includes the ECS out file, or file that is returned to the Provider/Vendor indicating whether a file has passed or failed.

TABLE OF CONTENTS

PREFACE	II
INTENDED USERS	II
MANUAL CONTENTS.....	II
PROBLEM RESOLUTION	1
REGISTRATION REQUIREMENTS	2
IDENTIFICATION CODES.....	2
SIGN UP PROCEDURES	2
<i>Sign up Overview.....</i>	<i>2</i>
<i>Documents</i>	<i>2</i>
<i>Purpose.....</i>	<i>2</i>
<i>Form 1 - Provider / Vendor Electronic Claim Submission Notification</i>	<i>4</i>
<i>Form 2 - Electronic Input Supplier Number, ID, and Password Application.....</i>	<i>7</i>
<i>Form 3 - Electronic Provider Agreement Form</i>	<i>10</i>
<i>Form 4 - Electronic Claim Data Authorized Signature Form.....</i>	<i>14</i>
<i>Form 5 – Vendors/Clearing Houses Submissions for AHCCCS Providers Form.....</i>	<i>17</i>
AHCCCS SECURED VPN CONNECTION SETUP GUIDE.....	19
INTRODUCTION.....	2
0	
DOWNLOADING NECESSARY FILES	21
INSTALLING THE VPN CLIENT	23
CONFIGURING THE VPN CLIENT	30
CONNECTING AND FTP BROWSING	34
ESTABLISH A VIRTUAL PRIVATE NETWORK (VPN) CONNECTION.....	34
USING FILE TRANSFER PROTOCOL (FTP)	35
<i>Microsoft Internet Explorer:</i>	<i>35</i>
<i>WS_FTP:</i>	<i>37</i>
<i>Command Line:</i>	<i>39</i>
DISCONNECTING THE VPN CLIENT	41
TROUBLESHOOTING	42
<i>'I cannot download the necessary files!'</i>	<i>42</i>
<i>'I cannot connect!'</i>	<i>42</i>
<i>'I have a personal firewall...is that a problem?'</i>	<i>42</i>
<i>'When I am connected to the VPN, is my computer secure and will it interfere with my current network?'</i>	<i>42</i>
<i>"How does the VPN work?"</i>	<i>43</i>
SUBMITTING CLAIMS ELECTRONICALLY TO AHCCCSA.....	44

FTP	44
<i>Production Directory Structure</i>	44
<i>Test Directory Structure</i>	44
COMMUNICATIONS SOFTWARE.....	45
SUBMISSION REQUIREMENTS	47
TRANSMISSION WINDOW.....	47
MINIMUM/MAXIMUM SUBMISSION.....	47
SUBMISSION FREQUENCY	47
TESTING	48
TESTING PROCEDURES	48
<i>Test File Submission</i>	48
<i>Testing Contact</i>	48
<i>Feedback</i>	48
TESTING REQUIREMENTS.....	48
<i>Number of Test Transmission</i>	48
<i>Transmission Volume</i>	49
<i>Test Identification</i>	49
<i>Additional Requirements</i>	49
ATTACHMENTS.....	50
REQUIRED ATTACHMENTS	50
NOTIFICATION PROCESS	51
FILE SPECIFICATIONS.....	52

PROBLEM RESOLUTION

Any problem encountered in the electronic submission of claims to the AHCCCSA should be directed to the AHCCCS Customer Support Center. ***Please note that this does not include any questions regarding this manual, or any issues, which may arise during the testing process.*** These questions should be directed to the Electronic Claims Submission Unit. Please see the *Testing* section of this manual for further information in this area.

AHCCCS CUSTOMER SUPPORT CENTER: (602) 417-4451

Please be prepared to supply the following information:

- Topic of call (“Electronic Claim Submission”)
- Name
- Organization
- Phone number
- Nature of problem (dial-up, receipt status, etc.)

This information will be logged, assigned a Ticket Number, and the Support Center will transfer you to the appropriate staff member to answer your question. If a staff member is not immediately available, your call will be returned as soon as possible. Please reference the Ticket Number assigned to your original call on any subsequent call to the Customer Support Center, which deals with the same issue.

The AHCCCS Customer Support Center should NOT be contacted for issues dealing with the testing process (receipt of claims, status of test, etc.) Please see the *Testing* section of this manual for further information on the testing process.

The AHCCCS Customer Support Center is staffed from 8:00 a.m. until 5:00 p.m. (Arizona time), Monday through Friday.

REGISTRATION REQUIREMENTS

Identification Codes

Assignment and maintenance of Identification Codes (User IDs, Electronic Supplier Numbers) and Passwords, required in the Submitting Claims Electronically to AHCCCSA section of this manual, will be the responsibility of the Electronic Claims Submission (ECS) Group, and will be communicated to the provider/vendor on the Electronic Input Supplier Number Application form discussed in the Sign up Procedures below.

Sign up Procedures

Sign up Overview

Before a Provider or Vendor can submit test and/or production electronic claims, AHCCCSA requires the completion of certain agreements, authorizations and control documents by the Provider or Vendor.

Documents

Forms 1 through 3 should be completed and returned to the Electronic Claims Submission Unit for processing (Form 3 should be signed and notarized). Form 4 should be completed and mailed to the AHCCCS Electronic Claims Submission Unit whenever Provider/Vendor personnel changes occur.

Form 1	<i>Provider/Vendor Electronic Claims Submission Notification</i>
Form 2	<i>Electronic Input Supplier Number Application</i>
Form 3	<i>Electronic Provider Agreement Form</i>
Form 4	<i>Electronic Data Authorized Signature Form</i>

Note: Forms 1 through 4 are submitted by the new Provider/Vendor to initiate electronic claims submissions, or by an existing Provider/Vendor, as applicable, when changes have occurred.

Purpose

The documents included in this section provide the following:

- An agreement specific to AHCCCSA and the Provider/Vendor for the submission, acceptance and processing of electronic claims.
- AHCCCSA with the names and signatures of Provider/Vendor representatives authorized to submit electronic data and sign related documents. The designated persons/parties will also be responsible to interact with the AHCCCS Electronic Claims Submission Unit.
- Authorization to process information electronically received by the AHCCCSA, and verify that it is accurate and complete.

Form 1

Provider / Vendor Electronic Claims Submission Notification

Form 1 - Provider / Vendor Electronic Claim Submission Notification

This document serves notice to AHCCCS Electronic Claims Submission Unit of the designated person authorized to receive information from AHCCCS regarding electronic claim submissions. It also furnishes an estimate of the number of claims to be reported. This notification form must be completed by Provider/Vendor before testing and submitting electronic claims data to AHCCCS.

Field No.	Instructions
1.	Enter the name of the Provider or Vendor.
2.	If applicable, enter the Provider ID number assigned by the AHCCCSA Administration.
3.	Enter the date the Provider/Vendor will begin submitting electronic claims to AHCCCSA.
4.	Monthly estimate of volume of HCFA-1500 claims that will be submitted to AHCCCSA.
5.	Monthly estimate of volume of UB-92 claims that will be submitted to AHCCCSA.
6.	Monthly estimate of volume of Universal Drug claims that will be submitted to AHCCCSA.
7-15	Enter the individuals' names to which the Provider/Vendor wants information sent regarding electronic claims.
16.	Enter the authorized signer name and title
17.	Enter the date the form was signed.
18.	Authorized signature/title.

Provider/Vendor Electronic Claim Submission Notification

1. Provider/Vendor Name: _____ 2. ID Number: _____

3. As a representative of the Provider/Vendor named above, I hereby notify the AHCCCS Administration that the Provider/Vendor electronic claim submissions will start on or about ____/____/____. Please allow at least 10 business days from the submission of this notification. The Provider/Vendor named above agrees to submit only clean electronic data, and correct any submission errors identified by the AHCCCS Administration.

The Provider/Vendor named above estimates that the monthly average/maximum electronic claim submission volume will be:

	Average	Maximum
4. HCFA-1500 Claims	_____	_____
5. UB-92 Claims:	_____	_____
6. Form C Claims:	_____	_____

The Provider/Vendor named above requests that electronic claim submission related information from the AHCCCS Administration be available to:

7. _____	8. _____
9. _____	10. _____
11. _____	12. _____
13. _____	14. _____
15. _____	

16. Authorized Representative/Title: _____ 17. Date: _____

18. Signature: _____

Form 2
Electronic Input
Supplier Number,
ID, And Password
Application

Form 2 - Electronic Input Supplier Number, ID, and Password Application

Upon receipt of a completed Electronic Input Supplier Number Application, a specific Supplier Number is issued

Field No.	Instructions
1.	Enter the name of the Provider/Vendor
2.	If applicable, enter the Provider ID number assigned to the provider by the AHCCCS Administration.
3.	Enter the Provider/Vendor street address.
4.	Enter the Provider/Vendor city, state, and zip code address.
5.	Enter the Provider/Vendor telephone number.
6.	Print the name of the Provider/Vendor contact person.
7.	Enter the Provider/Vendor contact's telephone and fax numbers.
8.	Enter the position title of the person authorized to act as signatory.
9.	Enter the name of the person authorized to act as signatory.
10.	Enter the signature of the person authorized to act as signatory.
11.	Enter the date the form was signed. Please allow 10 working days from the date of submission of this form for the number to be assigned by AHCCCS.
12.	Signature and title of the individual completing the form.

Electronic Input Supplier Number Application

1. Provider / Vendor _____ 2. Provider ID Number: _____

In order to submit electronic claims data to AHCCCS, Providers/Vendor must be assigned an electronic input supplier number. To apply for your supplier number, please complete the application below and forward to the AHCCCS Electronic Claims Submission Unit.

3. Provider/Vendor Address (Street): _____

4. City, State & Zip code: _____

5. Provider/Vendor Telephone/Fax Number: _____

6. Contact Person's Name: _____

7. Contact Person's Telephone Number: _____

8/9/10. Signature of Persons Authorized to act as Signers regarding electronic claims data.

Position	Name	Signature

11. Date: _____

12.
Signature: _____

For AHCCCSA Use Only. The following information will be completed by AHCCCSA and this form returned to the Provider/Vendor.

USER ID: _____ USER PASSWORD: _____
PROVIDER NAME: _____ ELECTRONIC SUPPLIER NO.: _____

Form 3
Electronic Provider Agreement
Form

Form 3 - Electronic Provider Agreement Form

The *Electronic Provider Agreement Form* is an agreement between the Provider/Vendor and AHCCCSA, which authorizes AHCCCS to accept claims data electronically. The agreement also holds the Provider/Vendor responsible for submitting this data in accordance with applicable Rules and Regulations, and within Electronic Claim Submission specifications.

Note: **This Document Requires Notarization By a Notary Republic.**

Field No.	Instructions
1.	Enter the name of the Provider/Vendor.
2.	Enter the date the form was signed.
3.	Enter the name of the Provider/Vendor.
4.	If applicable, enter the ID number assigned by the AHCCCS Administration.
5.	Signature of the individual authorized to act as signatory for the Provider/Vendor.
6.	Enter the day of the week the form is being notarized.
7.	Enter the month the form is being notarized.
8.	Enter the year the form is being notarized.
9.	Enter the name of the person authorized to sign documentation related to electronic claim submission.
10.	Notary Public name
11.	Notary Public signature
12.	Notary Public Seal

Electronic Provider Agreement Form

1. _____ (Provider / Vendor Organization, herein called “Provider”) hereby is authorized to submit claims data to the Arizona Health Care Cost Containment System Administration (hereafter called the “Agency”) for services rendered by the undersigned provider, in machine readable form, as specified by the Agency. The provider certifies that the claims data so recorded and submitted as input data are in accordance with all procedures, rules, regulations or statutes now in effect. If any of those procedures, rules, regulations or statutes are hereafter amended, the provider agrees to conform to those amendments of which the provider has been notified. Provider further certifies that it will retain and preserve all original documents as required by law, submit all or any part of same, or permit access to same for audit purposes, as required by the State of Arizona, or any agency of the federal government, or their representatives.

In consideration of the agency acceptance of the provider input data, the provider agrees to be responsible for any incorrect or delayed payments made to the provider as a result of any error, omission, deletion, or erroneous insert caused by the provider in the submitted data. In the event of any inconsistencies between the input data contained and underlying source documents, whether set forth in claim forms or otherwise, the Agency shall rely on the input data only.

The provider further agrees to hold the Agency harmless from any and all claims of liability (including but not limited to consequential damages, reimbursement of erroneous billings and reimbursement of attorney fees) incurred as a consequence of any such error, omission, deletion, or erroneous input data. The Agency shall not be responsible for any incorrect or delayed payments to the provider resulting from any error, omission, deletion or erroneous input that does not meet the standard prescribed by the Agency. Erroneous input data shall be returned to the Provider for correction and resubmission, within limited time frame prescribed by the Agency, at the Provider’s cost.

Electronic Provider Agreement Form

The Provider herewith authorizes the Agency to (1) make administrative corrections on submitted claims data to enable the automated processing of the same: and (2) accept as original evidence of services rendered, claim data in a form appropriate for automated data processing.

The Provider agrees and certifies that the provider's certification appearing on all claim forms in use as of a given submission date are incorporated by reference in this agreement, shall remain valid and applicable to all claim data submitted, and herewith are adopted by the Provider as though individually executed.

2. Date: _____

3. Authorized Provider Representative Name/Title: _____

4. Provider Number: (If applicable) _____

The undersigned is expressly authorized to sign for electronically transmitted claims data.

5. _____

Sate Of Arizona)
) ss
County Of)

6/7/8/9. On this _____ day of _____, 20 _____, before me personally came _____, to me known to be the individual described in and who executed the foregoing instrument, and he/she acknowledged to me that he/she executed the same.

10. _____
Notary Public

11. _____
Notary Public Signature

12. (Seal)

Form 4
Electronic Claim Data
Authorized Signature Form

Form 4 - Electronic Claim Data Authorized Signature Form

This form should be completed and mailed to the AHCCCS Electronic Claims Submission Unit when Provider/Vendor personnel changes occur. This form will serve as notification to AHCCCS of those individuals who are no longer authorized to submit or sign Electronic Claims Submission (ECS) documents on behalf of the Provider/Vendor.

Under no circumstances will AHCCCSA accept ECS documents from anyone other than the Provider/Vendor authorized signers.

Field No.	Instructions
1.	Enter the name of the Provider/Vendor.
2.	If applicable, enter the ID number assigned by the AHCCCS Administration.
3.	Enter the position title of the person authorized to sign ECS documents.
4.	Enter the name of the person authorized to sign ECS documents.
6.	Enter the name of the Provider/Vendor ECS contact person to be removed from authorization.
7.	Enter the day the contact person no longer be authorized to sign ECS documents.
8.	Name of the individual completing the form.
9.	Enter the date the form is signed.
10.	Signature and title of the individual completing the form.

Electronic Claim Data Authorization Signature Form

1. Provider / Vendor _____ 2. Provider ID Number: _____

The following individuals are authorized to sign Electronic Claim Submission documents for the above mentioned Provider/Vendor:

3/4/5.

Position	Name	Signature

The following individuals are no longer authorized to sign Electronic Claim Submission documents on behalf of the above mentioned Provider/Vendor:

6/7.

Name	Termination Date
	/ /
	/ /
	/ /

8. Completed by: _____ 9. Date: _____

10.
Signature/Title: _____

Form 5
Vendors/Clearing Houses
Submissions for AHCCCS Providers Form

Form 5 – Vendors/Clearing Houses Submissions for AHCCCS Providers Form

This form should be completed and mailed to the AHCCCS Electronic Claims Submission Unit when Vendors or Clearing Houses submit claims for AHCCCS Providers. This form will serve as notification to AHCCCS of those providers they will be submitting claims for.

Field No.	Instructions
1.	Enter the name of the Vendor or Clearing House.
2.	Enter the providers name.
3.	Enter the providers AHCCCS ID number.

Vendors/Clearing Houses Submissions for AHCCCS Providers Form

1. Vendor/Clearing House Name: _____

2. List of Provider Name (s):	3. Provider ID Number(s):

AHCCCS Secured VPN Connection Setup Guide

INTRODUCTION

Because of the increasing need for secure file transactions using common forms of internet connections, AHCCCS has incorporated the use of Virtual Private Networking.

What this means to external entities who are uploading/downloading files is; *all electronic transactions will be sent using encryption technology instead of clear-text over the Internet.*

To connect to AHCCCS for Electronic File Transmissions, you must meet the following prerequisites:

- Have Internet access - Dialup/Broadband through an Internet Service Provider (ISP) or High-speed through the use of a Local Area Network (LAN) *(NOTE: America Online is not supported)*
- A computer running Windows 95b or higher connected to that connection to the Internet
- Enough free space to install required software (at least 10MB)

Once you meet the prerequisites, you can proceed with the rest of this guide.

PLEASE READ THE ENTIRE GUIDE CAREFULLY BEFORE YOU BEGIN.

The guide will take you through the necessary steps, as defined in the table of contents:

1. Downloading the necessary files
2. Installing and configuring the VPN client program
3. Connecting to the AHCCCS network and using FTP
4. Logging off the VPN client

DOWNLOADING NECESSARY FILES

Open your web browser and go to: <ftp://vpn@www.statemedicaid.us>

NOTE:

If you receive a “Page cannot be displayed” message, perform the following steps to configure Microsoft Internet Explorer properly:

- Click on the Tools menu and then select “Internet Options”
- Click on the Advanced tab. Click the “Restore Defaults” button and then click OK
- Restart Microsoft Internet Explorer and try again
- If you still have problems, please read “I cannot download the necessary files!” in the TROUBLESHOOTING section.

When prompted, enter **vpn** for the username.

Enter the FTP download password that was included in your Electronic Input Supplier Authorization kit.

Click the LOGIN button.

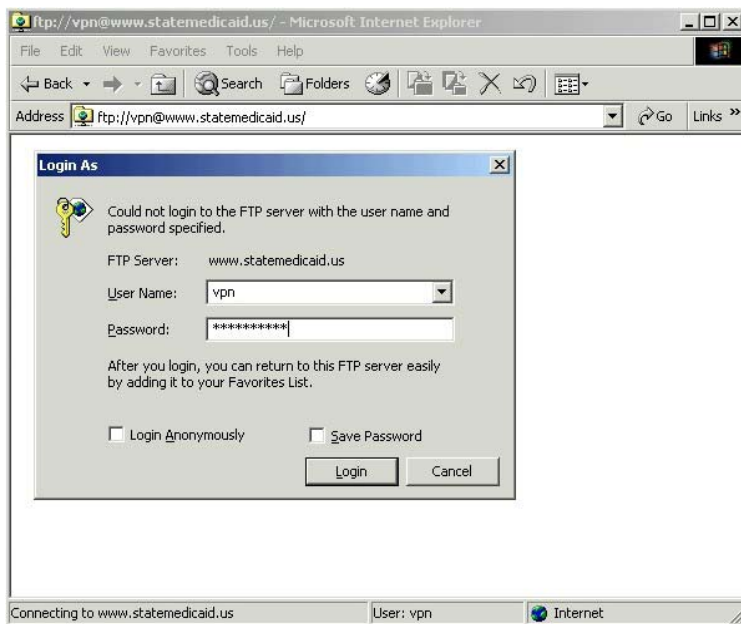


Figure 1.01 (FTP login for VPN download)

Right-click on **vpncclient-win-is-3.6.1.Rel-k-9.exe** and select “Copy to folder...”

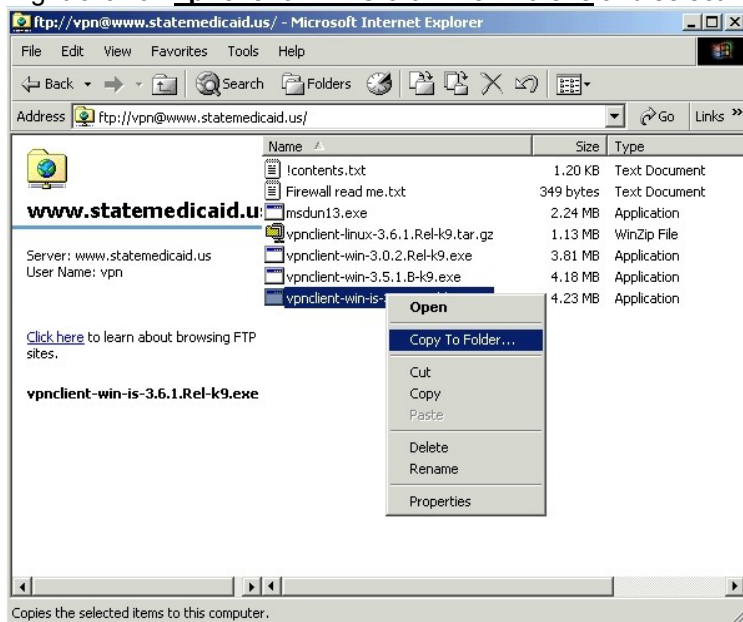


Figure 1.02 (Copy To Folder in MSIE)

NOTE:

The version compatibility list can be viewed within the !contents.txt file (double-click to view)

Browse to the Desktop and select OK.

The **vpncclient-win-is-3.6.1.Rel-k-9.exe** file will download to your desktop.



Figure 1.03 (Copy to Desktop)

INSTALLING THE VPN CLIENT

Locate **vpnclient-win-is-3.6.1.Rel-k-9.exe** on your desktop and double-click it. The WinZip Self-Extractor dialog box will appear.

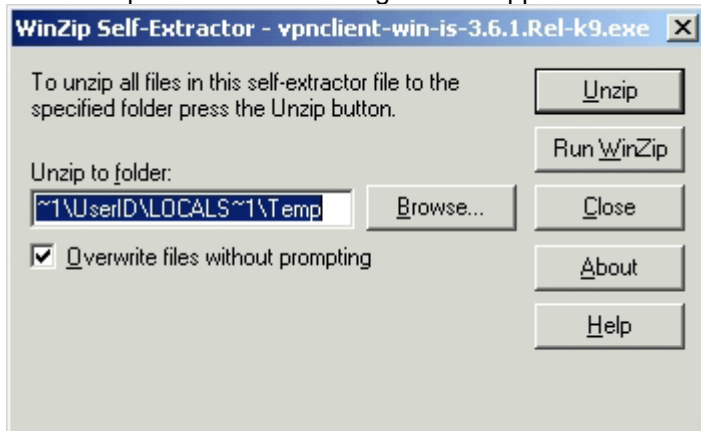


Figure 2.01 (Default WinZIP Extract Location)

Change the “unzip to folder” by typing in C:\VPN as shown below. Click the UNZIP button.

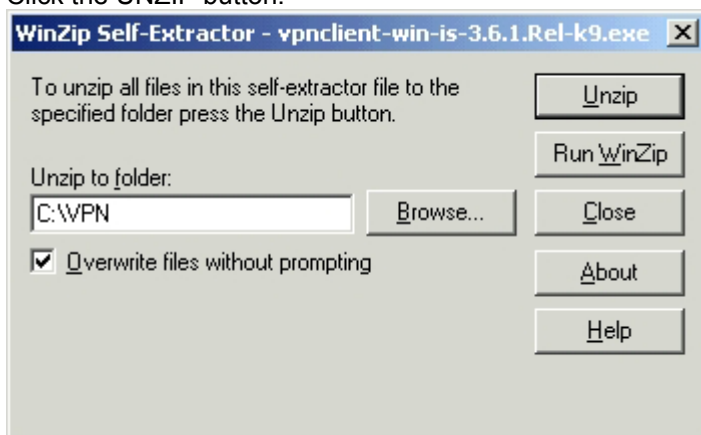


Figure 2.02 (Change Extract Location)

When all files are unzipped successfully, click the OK button.

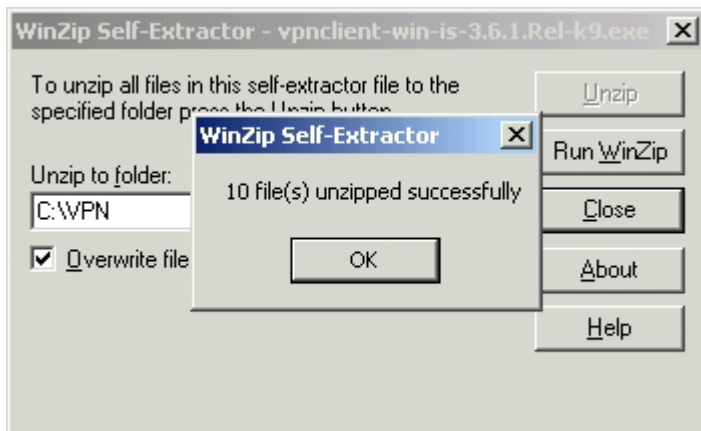


Figure 2.03 (Extract Complete)

Click the CLOSE button.

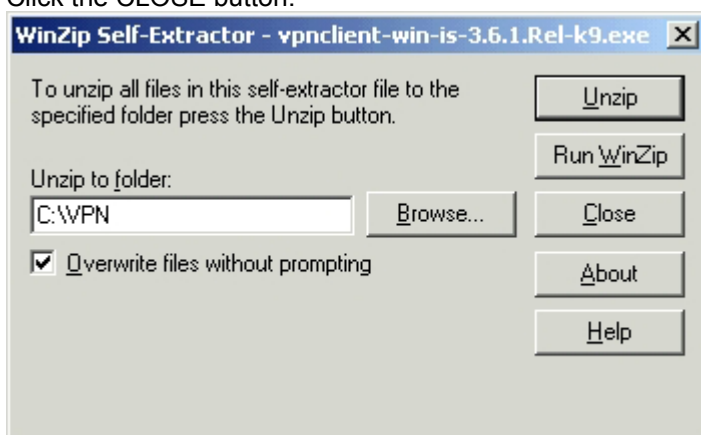


Figure 2.02 (Change Extract Location)

Browse with Windows Explorer to the newly created VPN folder located in the C: drive.
 (*Windows Explorer is access by going to Start | Programs | Windows Explorer)
 Double-click **Setup.exe**.

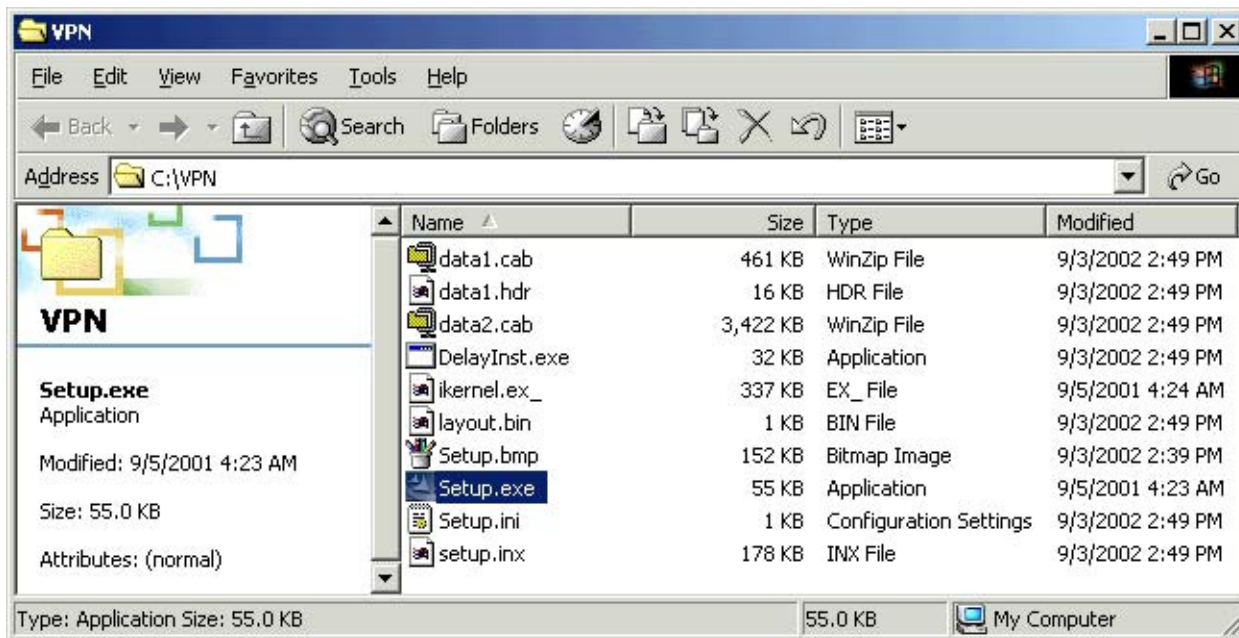


Figure 2.04 (Run Setup)

If prompted with the message below, click the YES button.

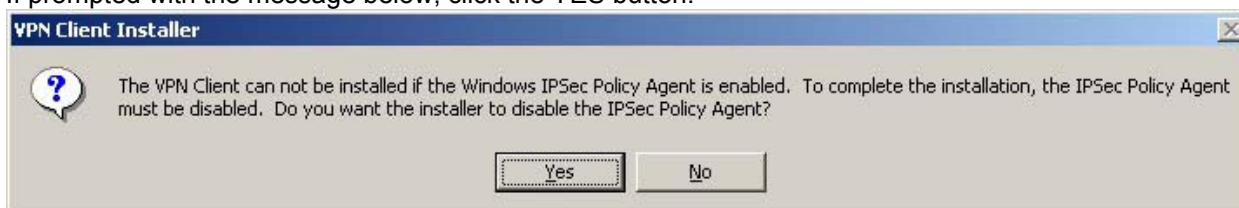


Figure 2.05 (IPSec Error)

Click the NEXT button to proceed.

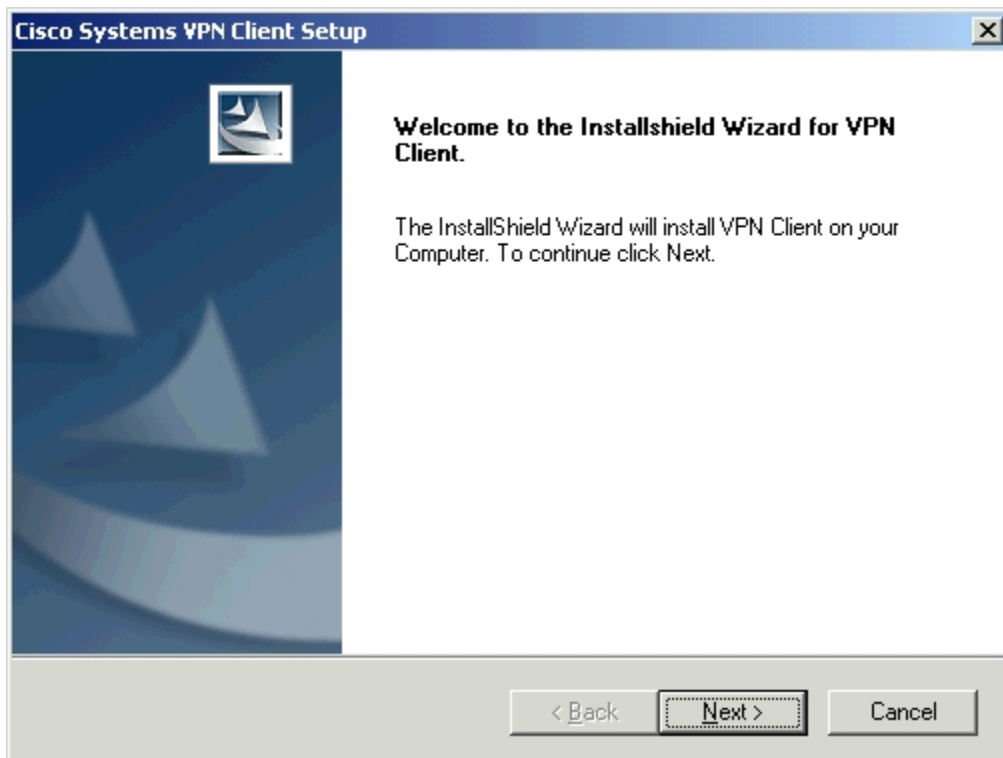


Figure 2.06 (Install Wizard Welcome)

Click the YES button to accept the license agreement.

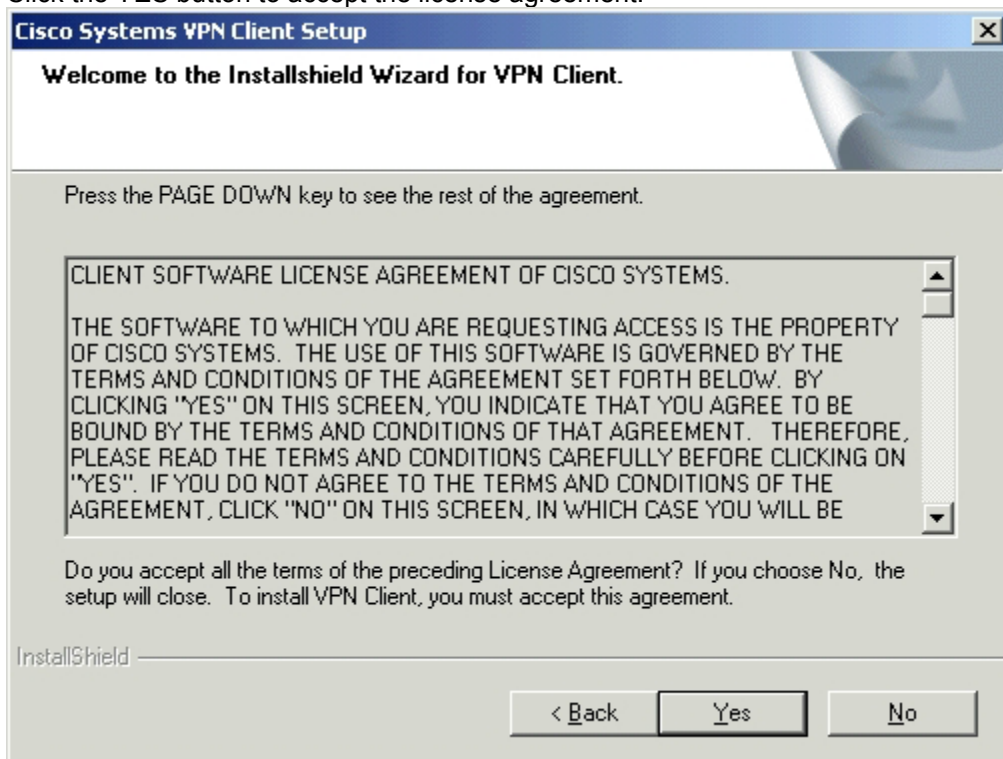


Figure 2.07 (Install Wizard License)

Click the NEXT button to accept the installation folder.

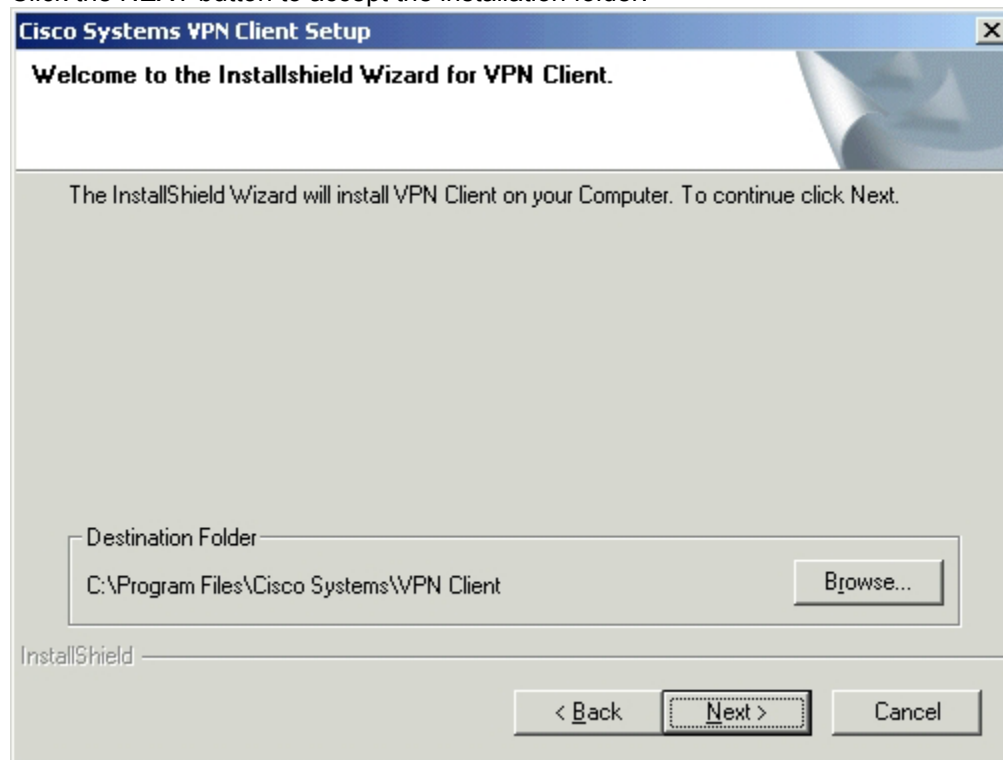


Figure 2.08 (Install Wizard Files)

Click the NEXT button to accept the Program Group.

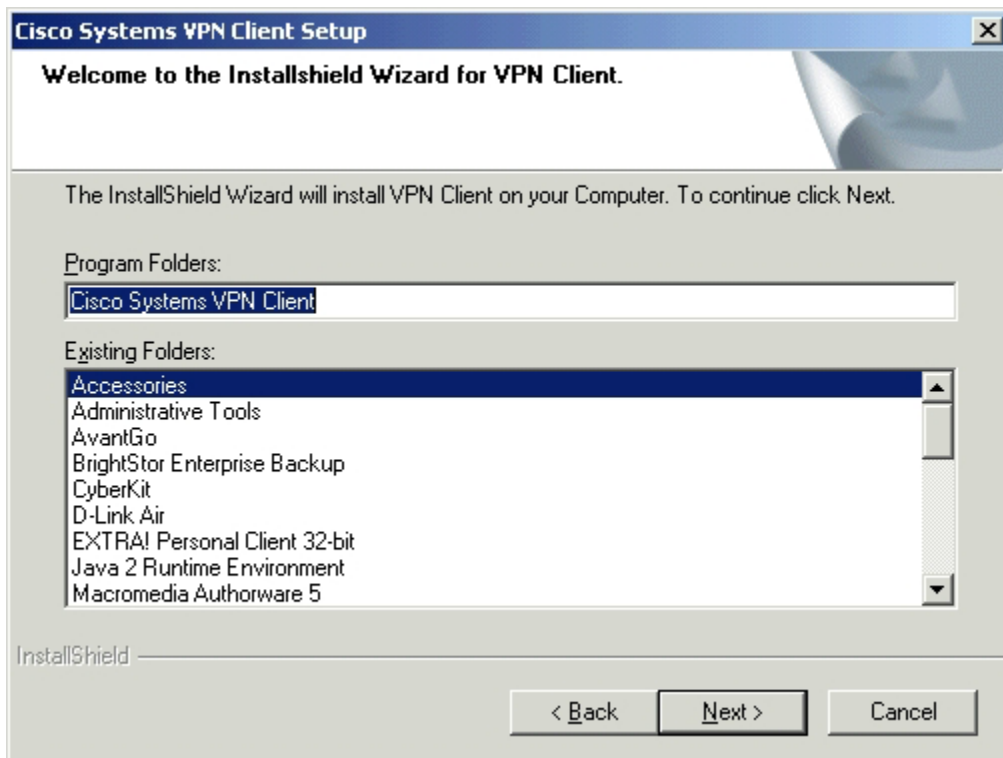


Figure 2.09 (Install Wizard Program Group)

Select 'YES, I want to restart my computer now' and then click the FINISH button.

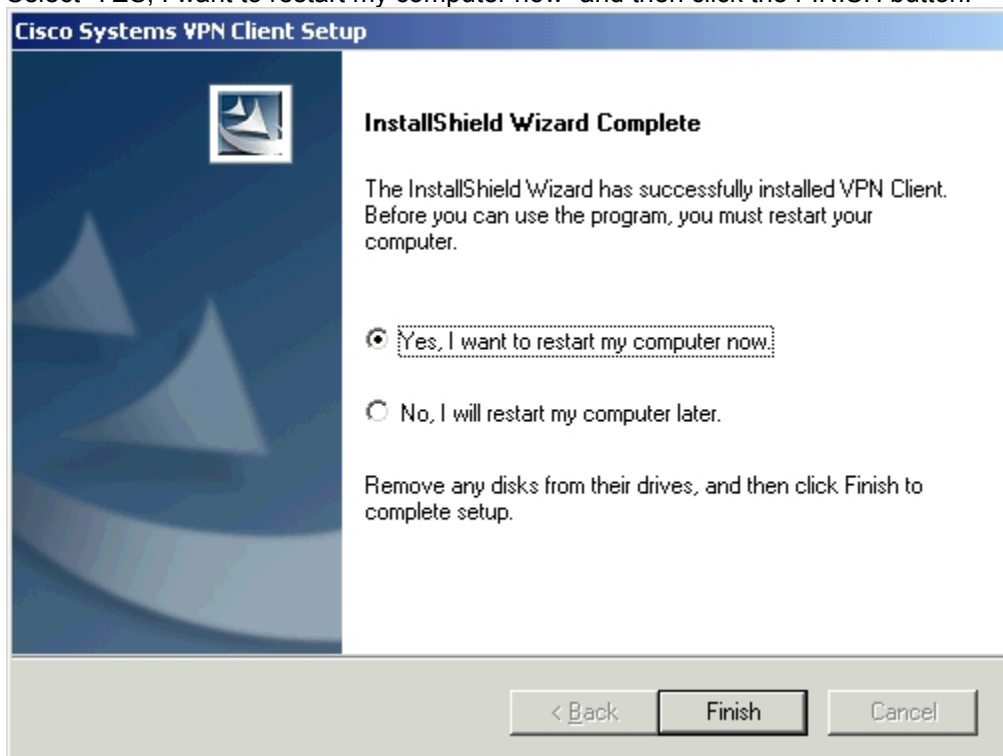


Figure 2.10 (Install Wizard Reboot)

The computer will reboot.

When the computer has finished rebooting, you can delete the **vpnclient-win-is-3.6.1.Rel-k-9.exe** file from your desktop. You can also delete the VPN folder located on your C: drive that was used for installation.

CONFIGURING THE VPN CLIENT

Click on **Start | Programs | Cisco Systems VPN Client | VPN Dialer** to launch the VPN Dialer program.

NOTE:

To make future use of the VPN Dialer more convenient, you can copy the “VPN Dialer” shortcut to your desktop.



Figure 3.01 (Start | Run)

Click the NEW button to configure a new Connection Entry.

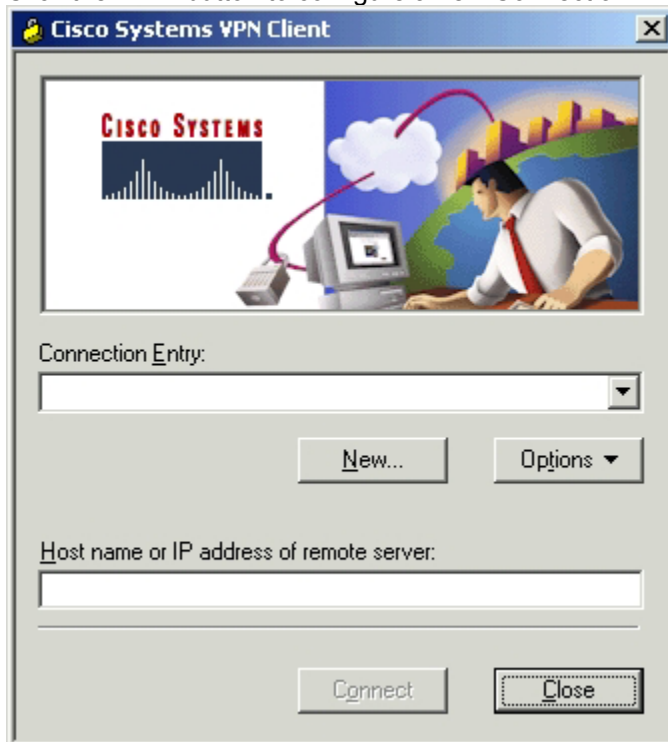


Figure 3.02 (VPN New Connection)

Enter the NAME information as shown below, and then click the NEXT button.



New Connection Entry Wizard

The VPN Client lets you create secure connections to remote networks. This wizard helps you create a connection entry for connecting to a specific remote network.

Name of the new connection entry:

Statemedicaid VPN

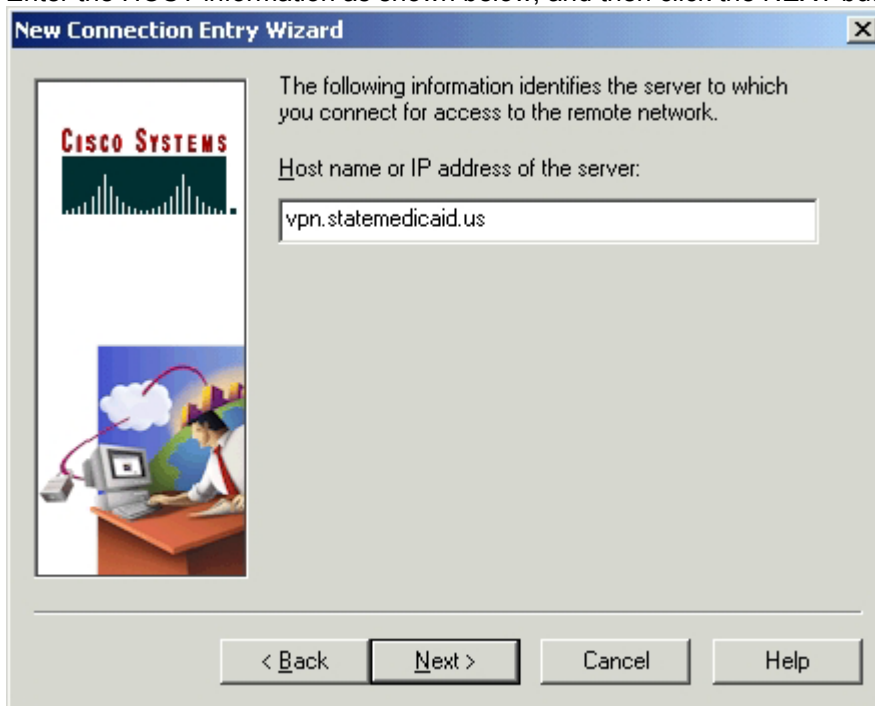
Description of the new connection entry (optional):

Secured Connection for Statemedicaid Systems

< Back Next > Cancel Help

Figure 3.03 (VPN New Name)

Enter the HOST information as shown below, and then click the NEXT button.



New Connection Entry Wizard

The following information identifies the server to which you connect for access to the remote network.

Host name or IP address of the server:

vpn.statemedicaid.us

< Back Next > Cancel Help

Figure 3.04 (VPN New Host)

Enter the GROUP information as shown below, and then click the NEXT button.

NOTE:

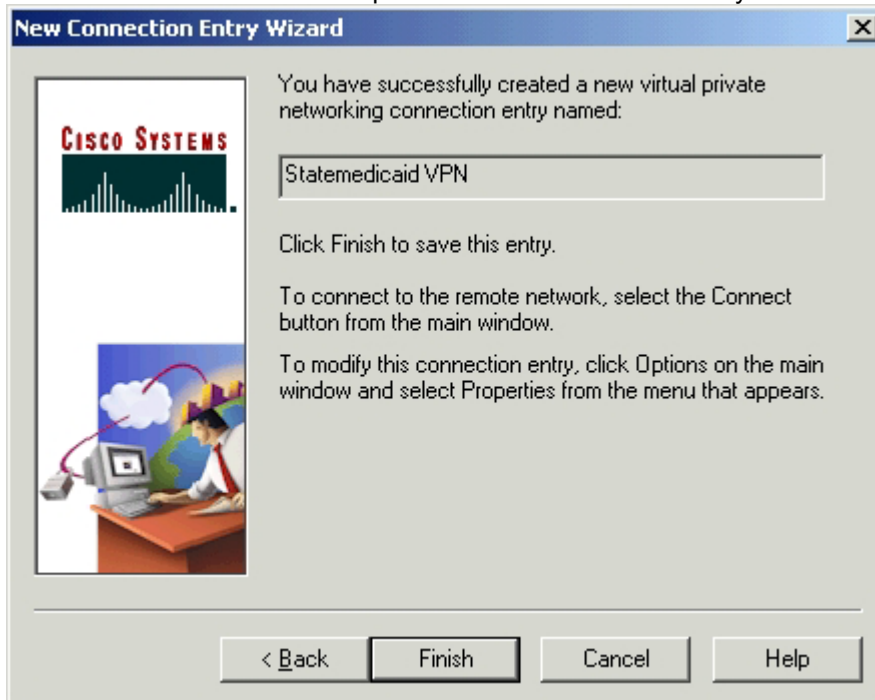
The password entered in this field will be the one supplied to you in the Electronic Input Supplier Authorization kit.



The screenshot shows the 'New Connection Entry Wizard' dialog box. On the left is a Cisco Systems logo and an illustration of a person at a computer. The main text area says: 'Your administrator may have provided you with group parameters or a digital certificate to authenticate your access to the remote server. If so, select the appropriate authentication method and complete your entries.' There are two radio buttons: 'Group Access Information' (selected) and 'Certificate'. Under 'Group Access Information', there are three text fields: 'Name:' with 'VPNFTP', 'Password:' with '*****', and 'Confirm Password:' with '*****'. Under 'Certificate', there is a 'Name:' dropdown menu showing 'No Certificates Installed' and a 'Validate Certificate...' button. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Figure 3.05 (VPN New Group)

Click the FINISH button to complete the New Connection Entry Wizard.



The screenshot shows the 'New Connection Entry Wizard' dialog box at the completion step. On the left is the same Cisco Systems logo and illustration. The main text area says: 'You have successfully created a new virtual private networking connection entry named:' followed by a text box containing 'Statemedicaid VPN'. Below this, it says: 'Click Finish to save this entry.' Then, it provides instructions: 'To connect to the remote network, select the Connect button from the main window.' and 'To modify this connection entry, click Options on the main window and select Properties from the menu that appears.' At the bottom are four buttons: '< Back', 'Finish', 'Cancel', and 'Help'.

Figure 3.06 (VPN Finished New)

Click the CLOSE button to exit the VPN Dialer program.

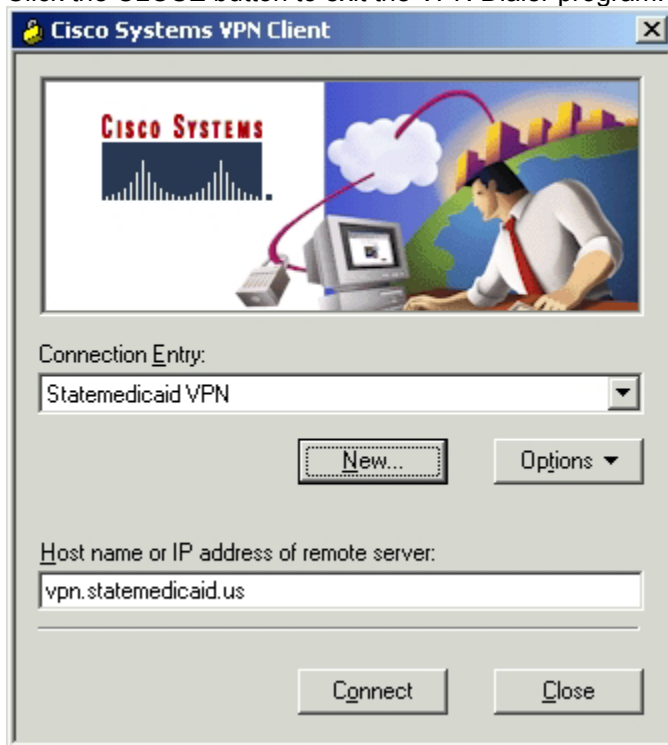


Figure 3.07 (VPN Connection Entry)

CONNECTING AND FTP BROWSING

Establish a Virtual Private Network (VPN) Connection

Click on **Start | Programs | Cisco Systems VPN Client | VPN Dialer** to run the VPN dialer program.



Figure 3.01 (Start | Run)

Click the **CONNECT** button to establish a VPN connection to the AHCCCS network.

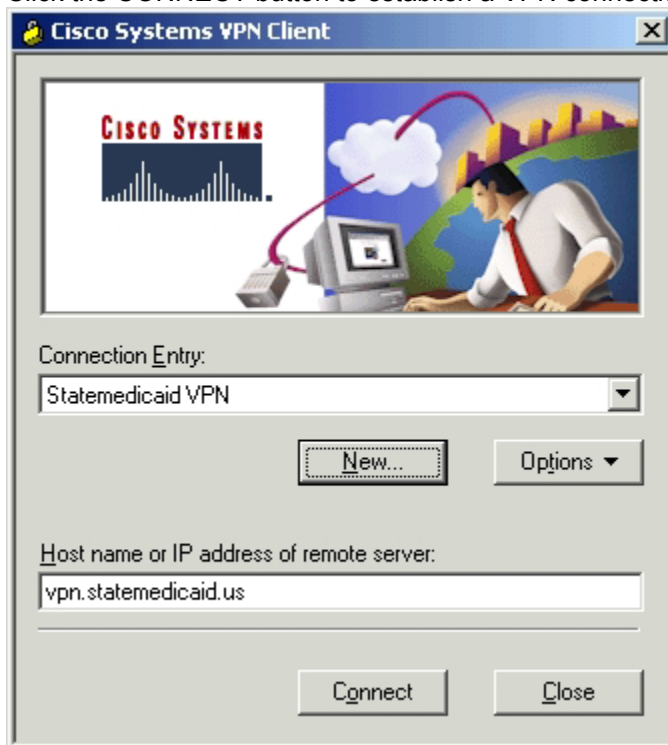


Figure 3.07 (VPN Connection Entry)

When you successfully connect, the dialog box below will display.
Click CONTINUE to proceed.

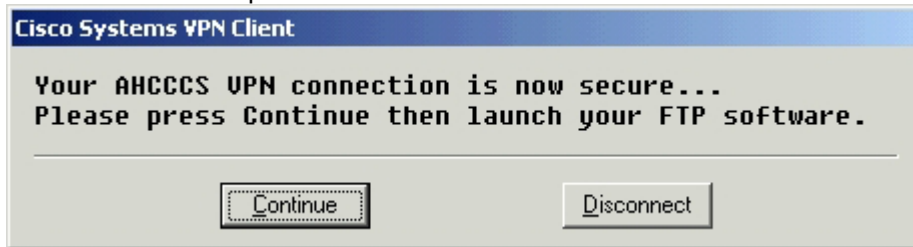


Figure 4.01 (VPN Connection Established)

To verify the connection, a yellow padlock should be visible in the bottom-right corner of your desktop (next to the system clock).

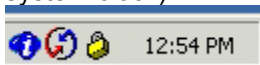


Figure 4.02 (VPN Dialer Confirmation)

Using File Transfer Protocol (FTP)

Once you have verified your VPN connection you can begin the file transfer process using your choice of FTP programs readily available. Once connected you can browse to your directory following the process outlined in the FTP Policy and Procedures Manual:

FTP/Submitter ID/System/Sub-system/Test, Prod/Data.txt (or Data.zip)

Below are examples of three, more popular, FTP programs that can be used for electronic file transactions.

Microsoft Internet Explorer:

Launch your Internet Browser and goto: <ftp://USERID@azftp.statemedicaid.us>

(where USERID is the user ID that was given to you upon registration)

You will be prompted for a **User Name**: (which should already have the ID you typed in) as well as a **Password**: (enter the one given to you upon registration).

Click **LOGIN**

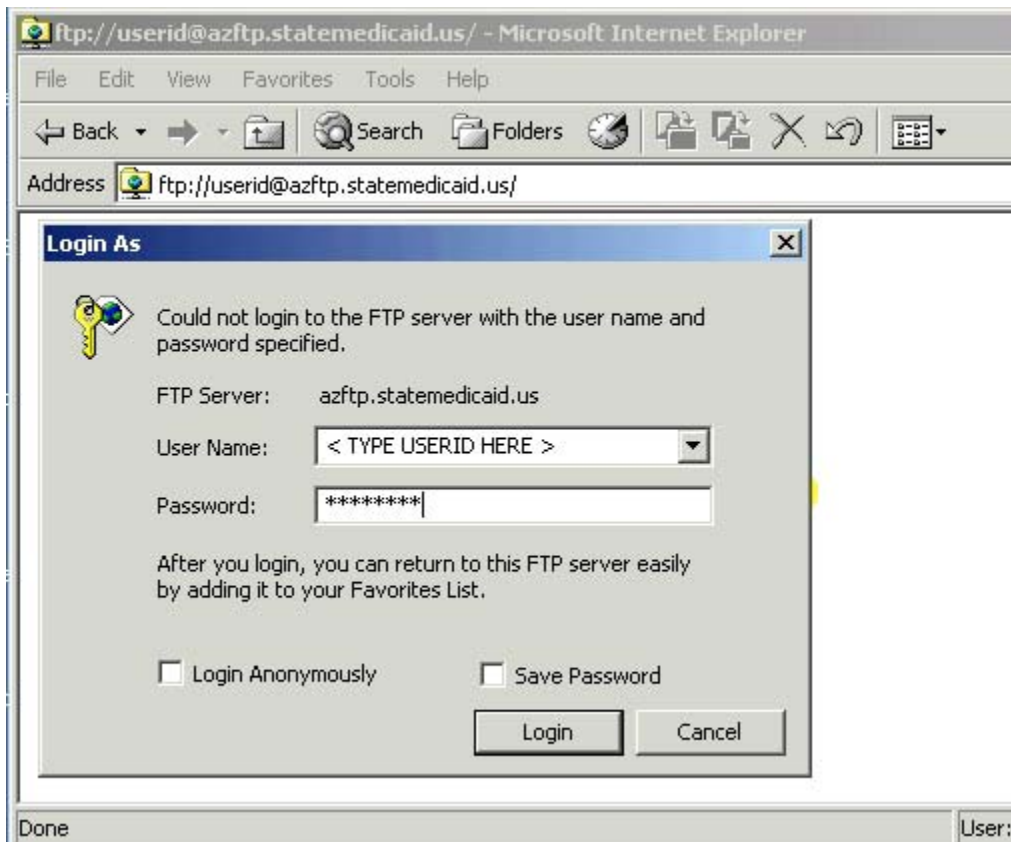


Figure 4.03 (FTP Browser to Host)

Once connected you can browse to the FTP directory and look for your submitter ID. Double-click on your directory and browse to the sub-folders that correspond to your task(s). From here you can drag-and-drop the file from your desktop (or hard drive) to the FTP Browser window.

Below is an example of a directory structure for Electronic Claims Submission

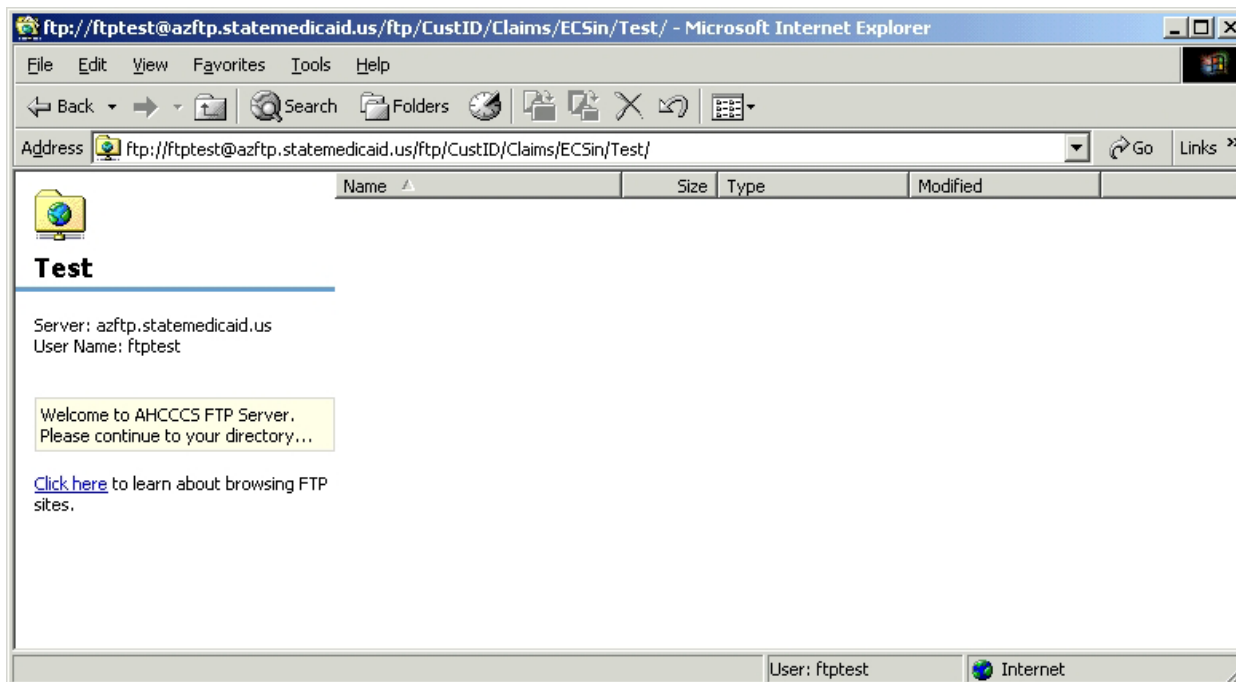


Figure 4.04 (FTP Browser Folder Structure)

WS_FTP:

Click on **Start | Programs | WS_FTP | WS_FTP95 LE** to run the FTP program.

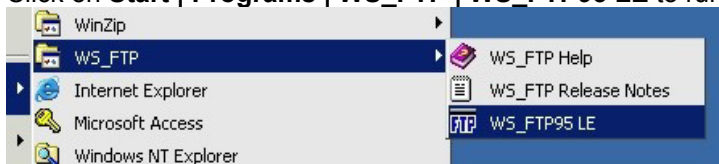


Figure 4.06 (Start WS_FTP)

Click the NEW button

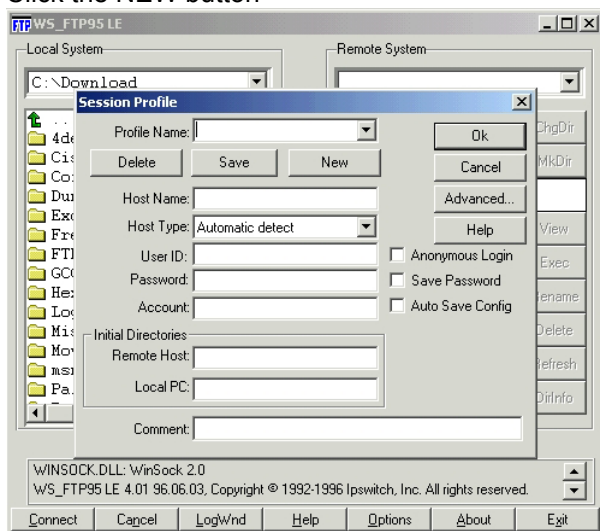
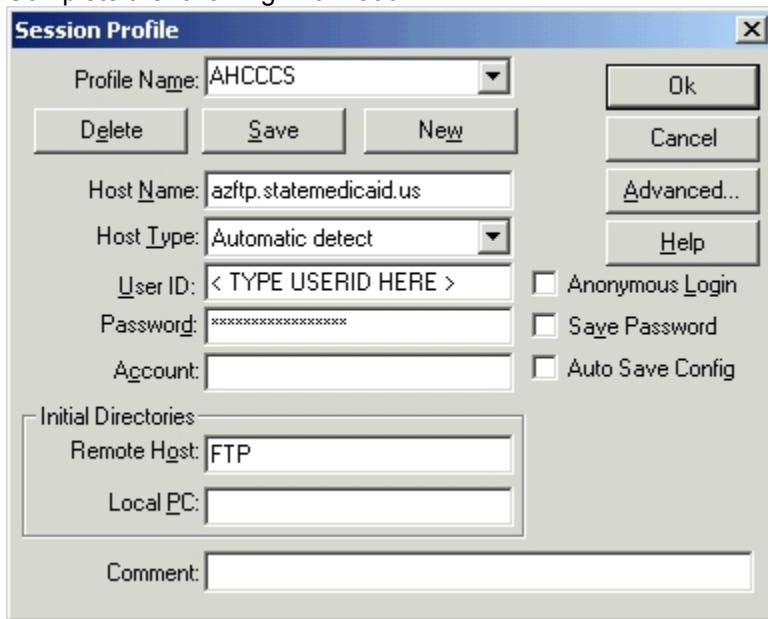


Figure 4.061 (FTP New)

Complete the following information



The image shows a 'Session Profile' dialog box with a blue title bar and a close button (X) in the top right corner. The dialog is organized into several sections. At the top, there is a 'Profile Name' dropdown menu with 'AHCCCS' selected. Below this are three buttons: 'Delete', 'Save', and 'New'. To the right of these buttons are 'Ok', 'Cancel', 'Advanced...', and 'Help' buttons. The main section contains fields for 'Host Name' (azftp.statemedicaid.us), 'Host Type' (Automatic detect), 'User ID' (< TYPE USERID HERE >), 'Password' (masked with asterisks), and 'Account'. To the right of these fields are three checkboxes: 'Anonymous Login', 'Save Password', and 'Auto Save Config'. Below these is a section titled 'Initial Directories' containing 'Remote Host' (FTP) and 'Local PC' fields. At the bottom is a 'Comment' text area.

Figure 4.062 (FTP Profile)

Replace <TYPE USERID HERE> with your **user ID** (which was given to you upon registration)

Type in password (which was given to you upon registration)

Click **SAVE**

Click **OK** (to start the connection)

Once connected browse to your directory (right half of window)

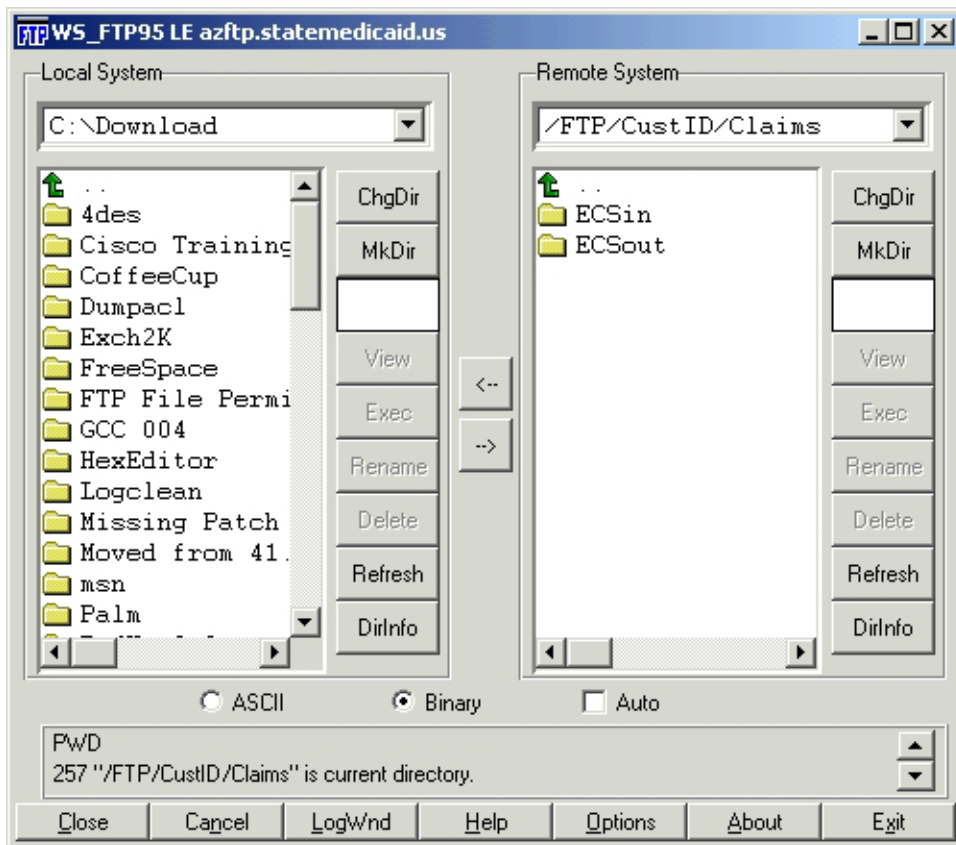


Figure 4.063 (FTP Browse)

Command Line:

Click **Start | Run |** type in **Command** and click **OK** to initiate the command line interface.

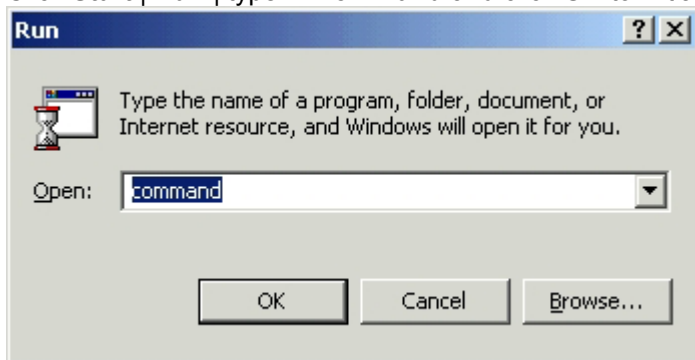


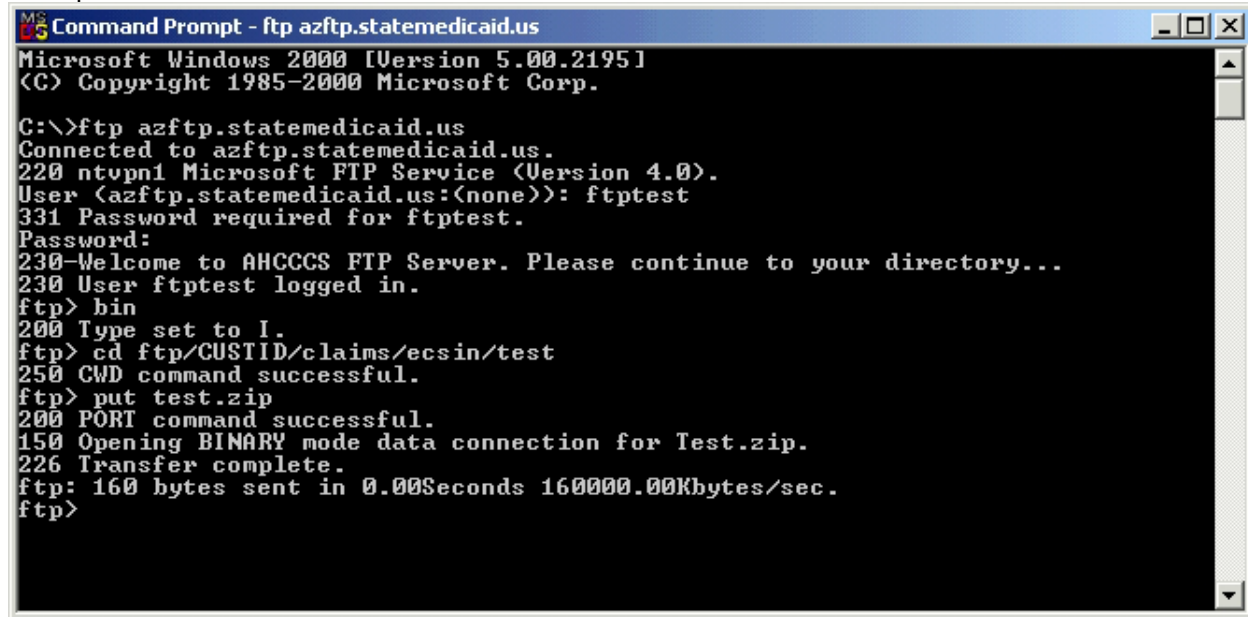
Figure 4.07 (Start | Run | Command)

At the C:\> type in the following commands:

1. Type in: **ftp azftp.statemedicaid.us** (to go to the FTP Host server)
2. Type in: **"USERID"** (where USERID is the user ID that was given to you upon registration)
3. Type in: **"password"** (given to you upon registration)
4. Type in: **bin** (to go to binary mode)
5. Type in: **cd ftp** (to change to the FTP directory)
6. Type in: **dir** (to give you a list of all the directories)

7. Type in: **cd "CUSTID"** (CUSTID is the submitter ID given to you upon registration)
8. Type in: **cd "Directories"** (to get to the system/sub-system directories)
9. Type in: **put "filename"** (to upload your files –optional)
10. Type in: **get "filename"** (to download your files –optional)

Example below:



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ftp azftp.statemedicaid.us
Connected to azftp.statemedicaid.us.
220 ntpn1 Microsoft FTP Service (Version 4.0).
User (azftp.statemedicaid.us:(none)): ftpptest
331 Password required for ftpptest.
Password:
230 Welcome to AHCCCS FTP Server. Please continue to your directory...
230 User ftpptest logged in.
ftp> bin
200 Type set to I.
ftp> cd ftp/CUSTID/claims/ecsins/test
250 CWD command successful.
ftp> put test.zip
200 PORT command successful.
150 Opening BINARY mode data connection for Test.zip.
226 Transfer complete.
ftp: 160 bytes sent in 0.00Seconds 160000.00Kbytes/sec.
ftp>
```

Figure 4.071 (FTP Commands)

- When finished, type in: **quit** (to close the FTP connection)
- Type in: **exit** (to close the command line interface)

DISCONNECTING THE VPN CLIENT

When you have finished with your session, right-click the padlock in the bottom-right corner of your desktop (next to the system clock) and select “Disconnect.”

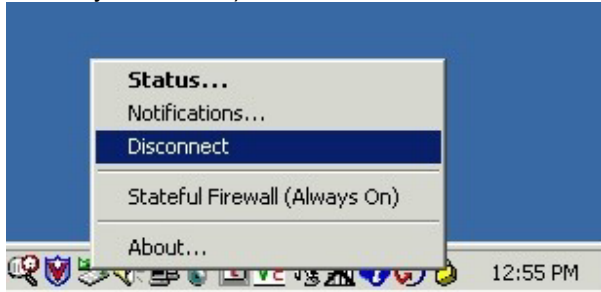


Figure 4.05 (VPN Disconnect)

TROUBLESHOOTING

‘I cannot download the necessary files!’

If you cannot download the necessary installation files with your web browser (especially if you use the AOL browser), you can attempt manually downloading the files as follows:

1. Bring up a DOS window -make note of where the prompt is... such as: **C:\>**
2. (If not at c, type in "cd <space> \") actual command is: **cd **
3. From the C:\> type in: **ftp www.statemedicaid.us**
4. If you're able to connect it'll prompt you for a user name
5. Type in: **vpn** for the user name
6. Password: *obtain FTP password from "Electronic Input Supplier Authorization kit"*
7. When it tells you that you are logged in, type in; **dir** (for a directory list)
8. Type in: **bin** (to go to binary mode)
9. Type in: **get vpnclient-win-is-3.6.1.Rel-k-9.exe** (to download VPN Dialer)
10. When finished type; **quit** then type: **exit** (to disconnect and close the window)
11. Go to your C: drive and locate files.
12. Refer to rest of this guide for installation and configuration instructions

‘I cannot connect!’

Before calling the helpdesk, you can perform some basic troubleshooting:

Reboot your computer and attempt to view a web page. If this works, proceed to the next step. If not, then work with your Internet Service Provider (ISP) to help trouble-shoot your Internet connection.

Are you able to get the yellow padlock in the bottom-right corner of your screen? This indicates you are connected to the VPN. If you see the padlock, proceed to the next step. If not, call the AHCCCS helpdesk with this information.

Are you able to connect to the FTP server? If not, what error message is preventing you from logging in? Record this information, and inform the AHCCCS helpdesk.

‘I have a personal firewall...is that a problem?’

Possibly. If you are having trouble connecting to the VPN or to the terminal server, try disabling your firewall, and then repeat the connection process. If you are then able to connect, the problem has been narrowed down to settings being too restrictive on your firewall. Refer to your firewall manufacturer's documentation for troubleshooting and configuration issues.

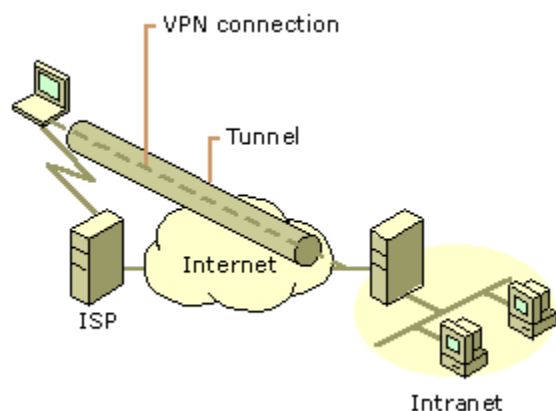
NOTE: This does not include large networks which might have a higher scale firewall system.

‘When I am connected to the VPN, is my computer secure and will it interfere with my current network?’

First, the quick definition from Microsoft's VPN Overview white paper:

"A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link."

“How does the VPN work?”



When the Tunnel has been created, the user's PC becomes an extension of the AHCCCS network - inheriting all security features of it. On the same token, when the connection is established, the user no longer has normal access to their own local area network because they are a part of the connected AHCCCS network. Since the VPN tunnel is encrypted at such a high level, you are blocked from all Internet traffic. Except for the encrypted tunnel, the chance of a security breach is virtually non-existent.

When connected to AHCCCS through VPN, your machine technically is not on the full network (it's not a member computer). Because of that, people here at AHCCCS are not able to get to your computer -or even see that it's participating with the network.

Communications Software

Following is a list of the software packages that have been evaluated, along with vendor contact information:

- RAS (Remote Access Server) Client for NT, which is included in Microsoft Windows/NT
- Dial-Up Networking for Windows 95, which is included in Microsoft Windows 95
- Trumpet Winsock Version 3.0 by Trumpet Software International Pty Ltd (Tested on Windows 3.11 only.)

Trumpet Winsock Version 3.0
<http://www.trumpet.com.au>
<ftp://ftp.trumpet.com>
Postal address:
Trumpet Software International Pty Ltd
GPO Box 1649
Hobart
Tasmania 7001
AUSTRALIA

- Cisco Remote by Cisco Systems, Inc. (Tested on Windows 3.11 only.)

Because AHCCCS' communication server was provided by Cisco, Cisco provides a partial version of this software, free, to be used only for communicating with the AHCCCS communications server. This product is called Cisco Remote Lite. AHCCCS will provide copies of this software on request, with the understanding that it is to be used only for communicating with the AHCCCS communications server.

Cisco Remote and Cisco Remote Lite
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA USA
800-553-NETS (6387) (In U.S. and Canada)
<http://www.cisco.com>

- WS_FTP

WS_FTP
Ipswitch Inc.,
333 North Ave.,
Wakefield, MA, 01880,
(617)-246-1150.
E-mail <info@ipswitch.com>.

- PC/TCP OnNet 1.1 & PC/TCP Network Software 3.0 by FTP Software, Inc. (This package includes both DOS and Windows versions. Only tested on Windows 3.11.)

PC/TCP OnNet 1.1 & PC/TCP Network Software 3.0
FTP Software, Inc.
2 High Street
North Andover, MA 01845
(508) 685-4000/http://www.ftp.com

Note that, of the software packages mentioned above, Trumpet Winsock and Cisco Remote Lite do NOT include FTP capability. (This capability is provided in the purchasable Cisco Remote product). There are several other FTP programs available from various vendors. One that has been evaluated and performs satisfactorily is WS_FTP by Ipswitch Inc.

SUBMISSION REQUIREMENTS

Transmission Window

Claims must be submitted between Midnight to 6:00 p.m. Monday through Thursday and Midnight to 4:00 p.m. on Fridays. Transmissions completely received by 6:00 p.m. on M-T and on by 4:00 p.m. on Friday will be loaded to the claims system on the day of receipt.

Minimum/Maximum Submission

A minimum of 1 claim must be included in each submission. This minimum is the count of claims, and not claim lines included in the transmission. The maximum submission requirement is 30, 000 per day per claim type, all submissions must be completely received by 6:00 p.m. Mon-Thurs and by 4:00 p.m. on Friday. Transmissions, which are not completely received by the allotted deadline, will not be accepted.

Submission Frequency

One transmission for each File type may be submitted by each submitting entity each day.

Testing Procedures

Each entity interested in submitting claims electronically using the methods outlined in this manual must successfully test prior to submitting production claims to AHCCCSA. All testing will be performed according to the following procedures:

Test File Submission

Test files will be submitted and named according to the directions in the *Submitting Claims Electronically to AHCCCSA* section of this manual. Claims must be submitted in the ASC X12N837 Claim Transactions format for professional, dental and institutional claims.

Testing Contact

The point of contact for all testing will be the Electronic Claim Submission (ECS) Unit (Division of Business and Finance). This unit may be reached at 417-4706 or 417-4892. The ECS Unit must be contacted prior to the submission of every test file. The type and number of claims being submitted should be communicated. The ECS Unit will coordinate all testing activities. This group is also responsible for granting production status to a submitting entity when testing has been successfully completed. Electronically submitted claims will not be accepted into production until this authorization has been granted.

Feedback

The results of each test will be communicated back to the submitter of the transmission by the ECS Unit. In addition, any expected system output such as a remittance advice, correspondence, etc. will be made available upon request. Please note that at this time, this information will not be available electronically.

Testing Requirements

The following testing requirements must be satisfied before any production electronic claims submission will be accepted by AHCCCSA. Each requirement must be met for each form type being submitted. As with the production requirement, different form types may not be submitted in a single transmission.

Number of Test Transmission

At least 2 submissions must be successfully received and processed, where success is defined as having a pre-edit acceptance rate of at least 95 percent. Pre-editing will verify that records are correctly sequenced and formatted, that all required (“R”) fields are present and correctly formatted, that all required if applicable (“I”) fields, if submitted, are correctly formatted, and that all required values are correctly coded.

Transmission Volume

Each successful transmission must contain at least 5, but no more than 25 claims, where a claim is defined, for testing purposes, as “claim line” for the 1500 and “claim” for the UB92.

At least 1 transmission with multiple providers (if submitter will be submitting for multiple providers) must be successfully received and processed.

Test Identification

Each test submission must be properly identified by coding the following fields:

Form Type	Field	Required Value
UB92	TEST/PROD INDICATOR (record type 01 position 178)	“T”
1500	TEST/PROD INDICATOR (record type AA0 position 254-257)	“TEST”
PHARMACY	TEST/PROD INDICATOR (record type BH position 254-257)	“TEST”

Please note that these values must be set to “P” and “PROD” respectively when submitting production claims.

Additional Requirements

At least 5 claims of the following types must be received and successfully processed:

- Other Adjustments (of previously submitted claims)
- Voids (of previously submitted claims)
- Medicare Insurance claims

All test claims must be valid AHCCCS claims. This means that, at a minimum, a valid AHCCCS member ID and provider ID must be on each claim. Actual (real life) service information is not a requirement, and for client confidentiality reasons, is not encouraged.

ATTACHMENTS

Since the electronic submission specifications contained in this manual do not allow for the submission of claim attachments, a process has been developed to process claims where additional documentation will be required by AHCCCSA in order to adjudicate the claim. Please note that ALL claims may be submitted electronically, regardless of attachment requirements. The AHCCCS claims system will determine if an attachment is required, and will send the submitter a letter identifying the type of attachment needed to adjudicate the claim. Claims will be held for 30 days until the requested attachments are received or whichever comes first..

Required Attachments

The following table identifies the claims which may require attachments, and which may not be adjudicated until the additional documents have been received. Documentation which was requested for a prior submission of a claim will not be required for any adjustments of that claim. Please refer to the *AHCCCSA Fee-For-Service Provider Manual* for complete information regarding required attachments. Where there are conflicts between this section and the Fee-For-Service Provider Manual, the Manual shall prevail.

Type of Claim	Required Attachment	Applicable Form Type		
		1500	UB-92	Form C
Non-Medical Documentation:				
IHS Recipient/Non-IHS Provider as applicable	IHS Referral	•	•	
Sterilization Service Diagnosis	Sterilization Consent Form	•	•	
Medicare/TPL	Explanation of Benefits (EOB)	•	•	
Medical Documentation:				
Claims that Require Medical Review*	Office Notes	•		
	Applicable Abortion Documentation	•	•	
	Trip Ticket	•		
	Operative (OP) Report	•	•	
	E/R Record		•	
	Itemized Statement		•	
	Admission Face Sheet		•	
	Admission History and Physical		•	
	Discharge or Interim Summary		•	
	Labor and Delivery Report		•	

* Please consult the *AHCCCSA Fee-For-Service Provider Manual* to determine which claims in these categories will require medical review.

** Prior Authorization Number may override certain attachments edit (IHS, Sterilization)

Notification Process

When a claim that has been electronically submitted requires additional documentation before it can be adjudicated, the provider will be notified of these requirements by letter. All attachments required to adjudicate a single claim will be contained in the same letter. The claim will then be aged, from the date of correspondence, for 30 days. If all attachments have not been received on the 30th day, the claim will be denied with an explanation indicating which documents were not received. Please note that all required attachments must be received within 30 days. Partial receipt of required attachments will not extend the 30 day window.

FILE SPECIFICATIONS

AHCCCSA follows the ASC X12N 837 Claim Transactions for professional, dental and institutional claims.

The HIPAA Transaction Companion Documents are available to electronic trading partners to clarify information on HIPAA-compliant electronic interfaces with AHCCCS. This document is available on our website at www.ahccs.state.az.us/HIPAA, under TCS documents.

Legend: **R**=Required / **O**=Optional / **N/A**=Not Applicable / **R/A**=Required if Applicable